



Številka: 007-53/2017/2 in 007-54/2017/2

Datum: 25. 7. 2017

Ministrstvo za notranje zadeve

Zadeva: Predlog Sporazuma med Republiko Albanijo, Republiko Avstrijo, Bosno in Hercegovino, Republiko Bolgarijo, Madžarsko, Republiko Makedonijo, Republiko Moldovo, Črno goro, Romunijo, Republiko Srbijo in Republiko Slovenijo o avtomatizirani izmenjavi podatkov o DNA, daktiloskopskih podatkov in podatkov iz registrov vozil in Pobuda za sklenitev Dogovora o izvajanju Sporazuma med Republiko Albanijo, Republiko Avstrijo, Bosno in Hercegovino, Republiko Bolgarijo, Madžarsko, Republiko Makedonijo, Republiko Moldovo, Črno goro, Romunijo, Republiko Srbijo in Republiko Slovenijo o avtomatizirani izmenjavi podatkov o DNA, daktiloskopskih podatkov in podatkov iz registrov vozil – mnenje Informacijskega pooblaščenca

Zveza: Vaš elektronski dopis z dne 20. 6. 2017 ter priloženo gradivo

Spoštovani,

v skladu z vašim zaprosilom z dne 20. 6. 2017 Informacijski Pooblaščenec (v nadaljevanju: IP) na podlagi prvega odstavka 48. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1; v nadaljevanju: ZVOP-1) podaja negativno mnenje k besedilu predloga Sporazuma med Republiko Albanijo, Republiko Avstrijo, Bosno in Hercegovino, Republiko Bolgarijo, Madžarsko, Republiko Makedonijo, Republiko Moldovo, Črno goro, Romunijo, Republiko Srbijo in Republiko Slovenijo o avtomatizirani izmenjavi podatkov o DNA, daktiloskopskih podatkov in podatkov iz registrov vozil (v nadaljevanju: predlog sporazuma), katerega namen je opredeliti pogoje in postopke za avtomatski prenos profilov DNK, daktiloskopskih podatkov in podatkov iz registrov vozil predvsem glede na to, da 25. člen predloga sporazuma določa, da pridržki k temu sporazumu niso mogoči. Nadalje predlagamo, da se v postopek priprave predloga Sporazuma nujno vključi tudi resorno ministrstvo za področje varstva osebnih podatkov, to je Ministrstvo za pravosodje. Mnenje velja v enaki meri za Pobudo za sklenitev Dogovora o izvajanju Sporazuma med Republiko Albanijo, Republiko Avstrijo, Bosno in Hercegovino, Republiko Bolgarijo, Madžarsko, Republiko Makedonijo, Republiko Moldovo, Črno goro, Romunijo, Republiko Srbijo in Republiko Slovenijo o avtomatizirani izmenjavi podatkov o DNA, daktiloskopskih podatkov in podatkov iz registrov vozil, zato v izogib podvajanju podajamo enotno mnenje za oba dokumenta.

V zvezi s tem izpostavljamo, da je Republika Slovenija ob ratifikaciji Konvencije o policijskem sodelovanju v jugovzhodni Evropi, ki je dejansko podlaga za sprejem predlaganega sporazuma, kot izhaja iz 3. člena Zakona o ratifikaciji Konvencije o policijskem sodelovanju v jugovzhodni Evropi (Uradni list RS - MP, št. 18/12 in št. 10/13; v nadaljevanju: MKPS), v skladu z 41. členom konvencije podala med drugim naslednji pridržek: »Republika Slovenija bo pogodbenici, ki ni država članica Evropske unije ali Evropskega gospodarskega prostora, posredovala osebne podatke, ki se obdelujejo ali se bodo obdelovali po opravljenem posredovanju, kot je določeno v 31. členu konvencije, ko državni nadzorni organ za varstvo osebnih podatkov, ustanovljen s skladu z zakonodajo Republike Slovenije, ob upoštevanju določb te konvencije o varstvu podatkov in na podlagi zakonodaje Republike Slovenije izda odločbo o skladnosti pravnega varstva osebnih podatkov te pogodbenice s pravili o varstvu osebnih podatkov, ki jih določa Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, in na njegovi podlagi sprejeta izvedbena zakonodaja Republike

Slovenije«. Iz tega sklepno že izhaja ugotovitev, da formalno zgolj določbe 31. člena MKPS ne zadoščajo kot zadostno zagotovilo za učinkovito zagotavljanje varstva osebnih podatkov po iznosu v tretje države, pogodbenice MPKS, ki niso članice EU ali Evropskega gospodarskega prostora. **Zdi se torej nerazumljivo, zakaj bi Republika Slovenija v zvezi z izmenjavo podatkov o DNA in daktiloskopskih podatkov, ki predstavljajo občutljive osebne podatke, ter podatkov iz registra vozil, na način, ki predvideva dostop do teh zbirk vsem državam pogodbenicam (ne gre torej za posredovanje podatkov na posamično zahtevo) znižala raven varstva glede na varstvo predvideno v MKPS.**

Upoštevajoč navedeno ni odveč pripomniti, da dejansko za številne izmed držav pogodbenic predloga sporazuma, ki niso članice EU, takšna odločba o ustreznosti varstva osebnih podatkov ne obstaja in da posledično torej dejansko niso izpolnjeni pogoji za iznos osebnih podatkov v te države. Glede na to se dejansko po našem vedenju osebni podatki z Republiko Slovenijo na podlagi navedene konvencije sploh še ne izmenjujejo. Zato se IP ob odsotnosti obstoja že določenih varovalk glede varstva osebnih podatkov, kot so opredeljene v MKPS, sprašuje o preuranjenosti sklepanja novih meddržavnih sporazumov in dogovorov o izmenjavi občutljivih osebnih podatkov na področju policijskega sodelovanja s tretjimi državami, ki sami po sebi ne vsebujejo ustreznih zagotovil o varstvu podatkov ob in po iznosu. Opozarjamo torej, da bi morali biti navedeni pridržki k MKPS v enaki meri upoštevani tudi pri sprejemanju predloga sporazuma in dogovora o njegovem izvajanju.

Navedeno velja tudi v skladu z novimi pravili varstva osebnih podatkov EU, ki že veljajo in se bodo začeli uporabljati maja 2018. Okvirni sklep Sveta 2008/977/PNZ z učinkom od 6. 5. 2018 dalje namreč razveljavlja Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ. Slednja prav tako v 35. členu ozko določa, da morajo države članice določiti, da pristojni organi vsak prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo, vključno z nadaljnjimi prenosi v drugo tretjo državo ali mednarodno organizacijo, *izvedejo samo, če je v skladu z nacionalnimi določbami, sprejetimi v skladu z drugimi določbami te direktive in samo če so izpolnjeni pogoji iz tega poglavja*, in sicer:

- (a) prenos je potreben za namene iz člena 1(1),
- (b) osebni podatki se prenesejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je organ, pristojen za namene iz člena 1(1),
- (c) v primeru prenosa ali omogočanja dostopa do osebnih podatkov iz druge države članice je zadevna država članica dala predhodno soglasje za prenos v skladu s svojim nacionalnim pravom,
- (d) Komisija je sprejela sklep o ustreznosti na podlagi člena 36 ali – v primeru, da Komisija ni sprejela tega sklepa – so predvideni ali obstajajo ustrezni zaščitni ukrepi v skladu s členom 37 ali – v primeru, da Komisija ni sprejela sklepa o ustreznosti na podlagi člena 36 ali ustreznih zaščitnih ukrepov na podlagi člena 37– se uporabljajo odstopanja za posebne primere v skladu s členom 38, in
- (e) v primeru nadaljnjega prenosa v drugo tretjo državo ali mednarodno organizacijo pristojni organ, ki je izvedel prvotni prenos, ali drug pristojni organ v isti državi članici dovoli nadaljnji prenos, potem ko ustrezno upošteva vse zadevne dejavnike, tudi resnost kaznivega dejanja, namen, za katerega so bili osebni podatki prvotno preneseni, in raven varstva osebnih podatkov v tretji državi ali mednarodni organizaciji, v katero se osebni podatki prenašajo v okviru nadaljnjega prenosa.

Nadalje direktiva določa, da države članice določijo, da so prenosi brez predhodnega soglasja druge države članice v skladu s točko (c) odstavka 1 dovoljeni samo, če je prenos osebnih podatkov nujno potreben, da se prepreči neposredna in resna grožnja javni varnosti v državi članici ali tretji državi ali vitalnim interesom države članice, predhodnega soglasja pa ni mogoče pridobiti pravočasno. O tem

brez odlašanja obvestijo organ, pristojen za dajanje predhodnega soglasja. Vse določbe tega poglavja se uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta direktiva.

Upoštevajoč navedeno in dejstvo, da 31. člen MKPS kot pogoj za začetek iznosov podatkov določa zgolj: da v zvezi z avtomatsko obdelavo osebnih podatkov, ki se sporočajo v skladu s to konvencijo, vsaka pogodbenica najpozneje z dnem začetka veljavnosti te konvencije sprejme potrebne notranje predpise, da bi dosegla raven varstva osebnih podatkov, ki je skladna z načeli Priporočila Odbora ministrov Sveta Evrope št. R (87) 15 z dne 17. septembra 1987 o uporabi osebnih podatkov v policijskem sektorju. Poleg tega je treba doseči raven varstva osebnih podatkov, ki je najmanj enaka tisti, ki izhaja iz Konvencije Sveta Evrope o varstvu posameznikov glede avtomatske obdelave osebnih podatkov z dne 28. januarja 1981. Osebnih podatki iz te konvencije se ne smejo sporočati, dokler na območjih pogodbenic, ki so vključene v tako sporočanje, ne začnejo veljati pravila o varstvu osebnih podatkov iz prvega odstavka. Za prenos podatkov skladno s prvim in drugim poglavjem te konvencije in za njihovo nadaljnjo uporabo in obdelavo pa 4. - 7. odstavek 31. člena MKPS določajo nekatere varovalke. Med drugim ima vsak pravico, da ga pristojni organ za obdelavo podatkov na njegovo zahtevo obvesti o podatkih, povezanih z njim, poslanih ali obdelanih v okviru te konvencije, ter pravico do popravka nepravilnih in do uničenja nezakonito pridobljenih podatkov. Izjeme od te določbe in praktični postopek pa so odvisni od notranje zakonodaje pogodbenice, ki se prosi za informacije, popravek ali uničenje. Gre torej za bistveno drugačne zahteve, kot jih vsebuje pridržek Republike Slovenije k MKPS.

Iz posredovanega predloga sporazuma prav tako **ni jasno razvidno, ali sploh in kako se ta predlog umešča v že izvedene aktivnosti v zvezi z izvajanjem MKPS, ki dejansko ne poteka učinkovito, predlog sporazuma pa govori poglobitvi čezmejnega policijskega sodelovanja v boju proti varnostnim grožnjam.** Če bi bili ti podatki znani, bi bilo mogoče ugotoviti, v čem je namen predloga novega sporazuma, torej zakaj sodelovanje opredeliti z dodatnim sporazumom, pri čemer MKPS očitno ni uspešno zaživela in v čem so pomanjkljivosti MKPS ter kako jih odpraviti. Na ta način bi bilo mogoče tudi oceniti potrebnost intenzivnejše obdelave osebnih podatkov (kot so predvidene s predlogom sporazuma) za opisane izredno široke namene.

V tej luči se IP, kot je dodatno pojasnjeno v nadaljevanju, zastavlja vprašanje ali je tak sporazum resnično potreben in skladen z določbami 117. člena Zakona o nalogah in pooblastilih policije, ZVOP-1 in Ustavo RS? Ne glede na to pa IP v nadaljevanju podaja svoje stališče tudi glede posameznih bistvenih vsebinsko najbolj spornih delov predloga sporazuma z vidika varstva osebnih podatkov.

1. Vključitev ustreznega pridržka glede zagotavljanja ustrezne ravni varstva osebnih podatkov, ki so predmet sporazuma

Predlog sporazuma se v uvodu sklicuje na s strani Republike Slovenije ratificirano Pogodbo med Kraljevino Belgijo, Zvezno republiko Nemčijo, Kraljevino Španijo, Francosko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko in Republiko Avstrijo o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije in Skupne izjave Kraljevine Belgije, Zvezne republike Nemčije, Kraljevine Španije, Francoske republike, Velikega vojvodstva Luksemburg, Kraljevine Nizozemske in Republike Avstrije k pogodbi z dne 27. 5. 2005 o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije (v nadaljnjem besedilu: Prümska pogodba)¹, Izvedbeni sporazum k Prümski

¹ Zakon o ratifikaciji Pogodbe med Kraljevino Belgijo, Zvezno republiko Nemčijo, Kraljevino Španijo, Francosko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko in Republiko Avstrijo o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije in Skupne izjave Kraljevine Belgije, Zvezne republike Nemčije, Kraljevine Španije, Francoske republike, Velikega vojvodstva Luksemburg, Kraljevine Nizozemske in Republike Avstrije k pogodbi z dne 27. 5. 2005 o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije (Uradni list RS – MP, št. 5/07 in št. 11/07).

pogodbi, Sklep Sveta 2008/615/PNZ z dne 23. junija 2008 o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (v nadaljnjem besedilu: Prümški sklep) in Sklep Sveta 2008/616/PNZ z dne 23. junija 2008 o izvajanju Sklepa 2008/615/PNZ o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (v nadaljnjem besedilu: Prümški izvedbeni sklep). IP poudarja, da gre v primeru t.i. Prümške pogodbe za akt, ki ureja sodelovanje med državami EU in se nikakor in v nobenem delu ne nanaša na sodelovanje med RS in tretjimi državami. Po mnenju IP primerov, kot je predlagani sporazum, Prümška pogodba ne ureja, niti sklicevanje nanjo, kot na enega od temeljev tega dogovora ni primerno. Razlog je poleg prvenstvenega, ki je povsem pravno formalne narave in po katerem pogodba ne veže strani, ki k njej niso in ne morejo pristopiti, predvsem v naravi povezave držav članic v okviru Evropske unije. Zakonodaja s področja varstva osebnih podatkov je namreč na ravni EU predmet harmonizacije (ki je od sprejema zakonodajnih aktov reforme prava EU za varstvo osebnih podatkov še na toliko višji ravni), kar pomeni, da je področna zakonodaja konsistentna v celotni Evropski uniji.

Za nadzor nad izvajanjem skupnih informacijskih sistemov (kot bi bile npr. nove zbirke podatkov o preiskavah DNA, ki bi jih za namen izvajanja predloga sporazuma vzpostavile morebitne pogodbenice sporazuma in zagotovile njihovo razpoložljivost drugim pogodbenicam) so na ravni EU oblikovana skupna nadzorna telesa s konkretnimi pristojnostmi. Enotnost prakse in razvoj pravnega področja se zagotavlja s skupnimi delovnimi skupinami (kot je npr. delovna skupina po členu 29 Direktive 95/46/ES **o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, v določenih primerih Evropski nadzornih za varstvo podatkov) od uveljavitve reforme z majem 2018 pa z novim Evropskim odborom za varstvo podatkov. V kontekstu predloga sporazuma, ki zajema tretje države pa ni mogoče govoriti o tovrstnih skupnih nadzornih osnovah na področju varstva osebnih podatkov v smislu skupnega nadzornega organa, ki bi lahko preverjal skladnost obdelave osebnih podatkov z dogovorom. Zaradi navedenega je sklicevanje na Prümško pogodbo in prenašanje njenih rešitev, ki veljajo znotraj EU, na ureditev med RS in tretjimi državami, po prepričanju IP povsem neprimerno in zavajajoče.**

Iz navedenega izhaja, da IP ni naklonjen predlaganemu načinu pridobivanja podatkov iz evidenc organov RS, po katerem bi bilo tretjim državam omogočeno povsem prosto elektronsko poizvedovanje o podatkih o prstnih odtisih, preiskavah o DNA² in registrih vozil.

2. Namen uporabe osebnih podatkov, ki so predmet izmenjave

IP poleg tega opozarja, da se predlagana rešitev kaže kot še posebej nesorazmerna glede na domet predloga sporazuma, ki vključuje tretje države. Sporazum se v uvodnih določbah sklicuje na zatiranje terorizma, čezmejne kriminalitete in nezakonitih migracij ter prizadevanja za izvajanje MKPS, pri čemer pa v zvezi z zbirko podatkov o preiskavah DNA 1. odstavek 1. člena predloga sporazuma kot namen določa preiskovanje kaznivih dejanj (torej vseh), 1. odstavek 3. člena pa tudi pomoč pri identifikaciji pogrešanih oseb. Pojem preiskovanje kaznivih dejanj se zdi po mnenju IP z vidika ustavno določenega načela sorazmernosti prekomeren oziroma nedoločen, saj pomeni, da dejansko lahko države pogodbenice same, s tem ko določijo določeno dejanje kot kaznivo in opredelijo obseg organov vključenih v preiskovanje ter začetek postopka preiskovanja, dejansko prosto širijo domet namena obdelave in izmenjave osebnih podatkov in nacionalnih zbirk osebnih podatkov policije.

Nadalje je v 5. členu predloga sporazuma kot namen zagotavljanja razpoložljivosti podatkovnih zapisov iz zbirke za nacionalne sisteme za avtomatsko identifikacijo prstnih odtisov opredeljeno

² Glede poizvedb v nacionalnih zbirkah podatkov o preiskavah DNK predlog sporazuma v 1. odstavku 2. člena določa, da pogodbenice vzpostavijo in vzdržujejo nacionalne zbirke podatkov o preiskavah DNA za namen preiskovanja kaznivih dejanj. Obdelava podatkov iz zbirk, vzpostavljenih po tem sporazumu, poteka skladno s tem sporazumom, MKPS in nacionalno zakonodajo, ki se uporablja za obdelavo podatkov. Na strani RS lahko hitro ugotovimo, da nacionalno pravo takšne obdelave osebnih podatkov (vzpostavitev dodatne zbirke o preiskavah DNA za namen izmenjave osebnih podatkov s tretjimi državami) ne dopušča.

preprečevanje (torej tudi neopredeljeno širok krog preventivnih aktivnosti) in preiskovanje kaznivih dejanj in pomoč pri identifikaciji pogrešanih oseb in neidentificiranih človeških ostankov.

Navedeno glede na terminologijo slovenske pravne ureditve področja kazenskega pregona pomeni, da gre za izmenjavo podatkov tako v fazi predkazenskega kot tudi kazenskega postopka in celo pred tem. To besedilo namreč dopušča zelo široke interpretacije, ki ne dajejo ustreznih zagotovil, da gre za sorazmerne posege v posameznikovo zasebnost. Prav tako pa je iz besedila sporazuma razvidno, da v 13. členu dovoljuje uporabo osebnih podatkov za katerikoli namen, če tako dovoli nacionalna zakonodaja pogodbenice prejemnice in je podano pooblastilo pogodbenice, ki upravlja zbirko podatkov, s čimer so popolnoma izničeni osnovni principi varstva osebnih podatkov posameznika³.

Vse to kaže na v določenih primerih nedopustno nedoločeno in širino namena obdelave osebnih podatkov, ki je dejansko od primera do primera prepuščen konkretnim okoliščinam. V skladu z veljavno evropsko in slovensko pravno ureditvijo tega področja, pa mora biti namen obdelave vnaprej jasno določen, v nasprotnem primeru obdelava osebnih podatkov ni dopustna. IP opozarja, da bi bilo v tem smislu potrebno jasneje, ožje in nedvoumno opredeliti, za katere namene je dopustno posamezne osebne podatke izmenjavati in naprej obdelovati v državi prejemnici. Ta namen mora biti jasno razumljiv ločeno od različne pravne ureditve kazenskega postopka in kazenskega pregona nasploh v posamezni državi pogodbenici sporazuma. Prav tako pa mora iz opredelitve namenov, za katere je izmenjava osebnih podatkov dopustna, izhajati, da so posegi v posameznikovo zasebnost v skladu s posameznimi nameni sorazmerni glede na cilje, ki jih posamezni namen izmenjave zasleduje.

3. Omejenost nabora osebnih podatkov, ki so predmet izmenjave

IP nadalje opozarja, da ni dopustna ureditev po kateri nabor osebnih podatkov, ki bi lahko bili predmet izmenjave, ni jasno in določno urejen. Tako 7. člen predloga sporazuma določa, da se v skladu z »nacionalno zakonodajo« določi pošiljanje nadaljnjih osebnih podatkov. To besedilo nakazuje na možnost izmenjave neznanega obsega osebnih podatkov poleg podatkov, ki so opredeljeni v 2., 5. In 9. členu predloga sporazuma, po prosti presoji vsakokratnih oseb, ki bodo podatke zahtevale oziroma posredovale, kar ni dopustno.

Prav tako pa IP opozarja, da nikjer v predlogu sporazuma ni izrecno določeno, da država prejemnica prejetih podatkov ne sme vključevati v svoje druge zbirke osebnih podatkov razen evidence na podlagi 2., 5. in 9. člena oziroma iz njih ustvarjati drugih novih zbirk. To bi lahko vodilo do primerov, ko bi se osebni podatki, ki bi jih RS posredovala drugim pogodbenicam, in nad katerimi ne bi imela kasneje nobenega vpliva oziroma nadzora, hranili neskončno dolgo za namene priprave in predložitve policijske prošnje ali sodnega zaprosila za pravno pomoč v skladu z nacionalno zakonodajo v najrazličnejših zbirkah.

4. Rok hrambe

IP nadalje opozarja na nedoločeno roka hrambe izmenjanih osebnih podatkov ter obveznosti brisanja osebnih podatkov, potem ko je namen izmenjave izpolnjen. Tako 12. člen predloga sporazuma določa, da se osebni podatki hranijo, do preteka najdaljšega roka za hrambo podatkov po nacionalni zakonodaji pogodbenice pošiljateljice, če je pošiljateljica na ta rok opozorila prejemnico, sicer pa se podatki zbršejo, ko niso več potrebni za namen, za katerega so bili poslani (ta pa je izredno širok). Ni torej opredeljen skrajni rok hrambe in dolžnost države prejemnice, da podatke dokončno briše. Glede na nejasnost namenov uporabe osebnih podatkov, ki so predmet izmenjave, bi bila namreč na podlagi obstoječega besedila možna tudi interpretacija, po kateri se podatki lahko hranijo dejansko zelo dolgo oz. brez časovnih omejitev.

³ Kot na primer možnost nadzora obdelave osebnih podatkov s strani posameznika tudi z zahtevo po seznanitvi z lastnimi osebnimi podatki, obdelavo osebnih podatkov le za namene, ki jih določa pravni temelj in so posamezniku vnaprej znani, načela minimizacije in sorazmernosti pri obdelavi osebnih podatkov.

5. Pravica posameznika do seznanitve z lastnimi osebnimi podatki in do popravka ter izbrisa

Pravica posameznika do seznanitve z lastnimi osebnimi podatki je po 18. členu predloga sporazuma omejena z nacionalno zakonodajo. To omogoča teoretično nedopustno situacijo, v kateri bi se lahko znašel posameznik, katerega podatke bi Republika Slovenija posredovala izven EU ali Evropskega gospodarskega prostora.

Enako velja za pravico posameznika do popravka ali izbrisa osebnih podatkov, v skladu s katero ima posameznik, na katerega se nanašajo osebni podatki, možnost, da zahteva dopolnitev, popravek, blokado ali izbris za tiste osebne podatke, za katere dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom, saj se to izvaja v skladu z nacionalnim pravom pogodbenice prejemnice, torej ne nujno pravom EU oz. RS.

Podobna velika odstopanja je najti tudi v drugih določilih predloga sporazuma, zato IP poudarja, da je sporazum v predlagani obliki posledično tudi dogovor o njegovem izvajanju z vidika zagotavljanja ustrezne ravni varstva osebnih podatkov za Republiko Slovenijo nesprejemljiv. Zgolj občasno sklicevanje na nacionalno pravo države pogodbenice upoštevajoč določila predloga sporazuma ne daje ustreznih zagotovil, da bo posameznikom, katerih podatki bi bili lahko predmet izmenjave zagotovljena ustrezna raven varstva osebnih podatkov, kot jo predvideva Ustava RS.

S spoštovanjem,

Pripravila:
Alenka Jerše, univ. dipl. prav.,
namestnica informacijske pooblaščenke

Mojca Prelesnik, univ. dipl. prav.,
Informacijska pooblaščenka